Indice

1. NUOVI SOCI

Hanno aderito al CLUSIT le seguenti organizzazioni:

- Banca Carige (Genova),
- Wireless (Milano).

2. CYBERCRIME

Sollecito al pagamento di fatture.

Mentre stiamo andando "in stampa" il nostro laboratorio di Phishing ci avverte che sono in arrivo email, anche in italiano, che richiedono il pagamento di fatture.

Come anche avverte il sito della Polizia di Stato (commissariato on line) se ci si collega al sito viene scaricato un virus.

Le email cominciano ad essere di buona fattura (trattandosi di una...fattura!).

E' bene ricordare al personale dell'azienda di non aprire email il cui mittente è sconosciuto.

Un problema non indifferente è per quei cittadini che accedono ad internet dal personal computer di casa e che, avendo tra l'altro contatti con l'estero, possono cadere più facilmente nella trappola ed aprire le email truffaldine. Così facendo, si infettano il computer e il criminale può catturare informazioni riservate, alcune delle quali possono riguardare i rapporti con una banca.

Dato che il rischio che il Cliente, collegandosi poi al servizio di Home Banking della sua banca, possa così trasferire al criminale, tramite il virus, le sue credenziali, ANSSAIF insiste nella necessità che ci siano iniziative ed investimenti, da parte delle Istituzioni, nella creazione della giusta conoscenza e sensibilità nei confronti dei pericoli.

Una giusta sensibilizzazione deve partire dalla favola di cappuccetto rosso ed illustrare che i pericoli di impersonificazione sono vecchi come il mondo (ci sono altri esempi, basta scegliere); si deve poi spiegare che rispondere al telefono, o alla posta, o al computer a sconosciuti, così come aprire loro la porta, significa poter incorrere in gravi pericoli.

L'attività svolta dalle associazioni dei consumatori è indispensabile e va assistita. Ma non basta da sola. Il mondo criminale si va incattivendo e creando sistemi sempre più sofisticati.

Il consumatore deve divenire ancora più furbo. O, almeno, se ha dubbi, chiamare la propria banca, o l'emittente la carta di credito, oppure, la Polizia e chiedere spiegazioni e consigli.

Ovviamente, non ci stancheremo mai di sollecitare i soci, che ricoprono incarichi di responsabilità nella Sicurezza, di proseguire incessantemente nella loro azione di prevenzione. Con l'occasione ricordiamo che ANSSAIF rimane convinta che organizzazioni criminali possono aver installato malware nei computer aziendali e raccolto informazioni utili per un eventuale attacco.

Troppi segnali portano in quella direzione. Specialmente le aziende che operano in certi settori è bene che rafforzino le difese.

Fonte: ANSSAIF - Associazione Nazionale Specialisti Sicurezza in Aziende di Intermediazione Finanziaria - www.anssaif.it

3. HACKER'S PROFILING PROJECT

Nel mese di Settembre, CLUSIT ha deciso di sostenere il progetto **HPP *Hacker's Profiling Project***, un progetto di ricerca internazionale ed open-source dell'ISECOM (Institute for Security and Open Methodologies).

Il CLUSIT collaborerà alla disseminazione dei risultati del progetto di ricerca e all'awareness verso quelle organizzazioni che ne facciano richiesta.

Segue un riassunto del progetto HPP.

Introduzione

In questi ultimi anni si è verificata una serie di fenomeni, che possono essere definiti come “preoccupanti” sotto diversi punti di vista: escalation del phishing, azioni di web-defacement, frodi e truffe economiche, attacchi ad infrastrutture di telecomunicazione pubbliche e private, azioni di hacking verso strutture governative.

Nello specifico, si è innanzitutto registrata una diminuzione della c.d. “window of exposure”, ovverosia del tempo che trascorre dalla stesura di un exploit “0-day” – circolante esclusivamente all’interno di un ristretto giro di persone – sino al loro utilizzo in attacchi massicci e/o distribuiti a livello mondiale; in secondo luogo, è poi da evidenziare l'esistenza di pericolose sinergie tra personalità tecnologicamente avanzate, criminalità organizzata e terrorismo, oltre alla continua crescita della interdipendenza tra la stabilità nazionale (infrastrutture critiche nazionali, homeland security,telecomunicazioni, servizi di base, etc.) e le problematiche di ICT Security.

Ciò nonostante, spesso i fenomeni del cybercrime e degli hi-tech crime vengono analizzati in maniera errata, focalizzando gli sforzi su attaccanti di poca rilevanza e basso impatto tecnologico, perdendo invece il controllo su agenti di minaccia di medio ed alto livello.

Con il progetto H.P.P. si vuole quindi analizzare il “problema del cybercrime” utilizzando un approccio completamente diverso da quelli individuati sino ad oggi, andando cioè direttamente alla fonte.

Obiettivi della ricerca

Il progetto H.P.P. si pone l’obiettivo di:

- Analizzare il fenomeno dell’hacking nelle sue mille sfaccettature – tecnologico, psicologico, sociale ed economico, mediante approcci sia di tipo tecnico che criminologico;
- Individuare gli attori chiamati in causa e comprenderne le effettive (e differenti) motivazioni;
- Osservare “sul campo” le azioni criminali;
- Applicare ai dati raccolti la metodologia di profiling elaborata;

- Apprendere dalle conoscenze acquisite e divulgarle.

È infatti essenziale, per i professionisti del settore, sia per chi si occupa di sicurezza informatica sia per gli investigatori o gli agenti governativi che devono indagare su casi di intrusioni informatiche, *sapere con chi hanno a che fare*. Questo sia al fine di adottare tutte le contromisure necessarie per rendere più sicuro i sistemi informativi e le infrastrutture di telecomunicazione, ma anche per identificare con maggiore rapidità l'autore dell'intrusione e, soprattutto, evitare di prendere le classiche “lucciole per lanterne”, come spesso accade nelle operazioni di computer-crime.

Oltre ad agevolare le finalità repressive verso azioni criminose di computer crime, lo studio consentirà anche di adottare misure preventive. Si pensi, infatti, ad un potenziale target il quale, se consapevole del tipo di attacco cui è più probabilmente soggetto e di quale agente di minaccia (ovverosia la tipologia di attaccante) è oggetto di preferenza, potrà *adottare tutte quelle misure* volte a ridurre il rischio di una possibile intrusione.

Elementi innovativi della ricerca

La novità dello studio consiste nell'interdisciplinarietà, in quanto coniuga la criminologia con la sicurezza informatica, al fine di individuare le diverse tipologie di hacker, considerando: le modalità di azione (da solo/a o in gruppo), le capacità tecniche, le motivazioni, gli scopi, i target, l'adesione o meno alla c.d. “etica hacker”.

Per maggiori informazioni rimandiamo ai siti:
www.clusit.it/pres/lugano110406rc.pdf
www.isecom.org/hpp
http://hpp.hackinthebox.org

Referente del Progetto, per conto del Clusit, è Raoul Chiesa, membro del Comitato Direttivo e del Comitato Tecnico Scientifico, che risponderà alle richieste di approfondimento ed eventualmente di collaborazione, da inviare a rchiesa@clusit.it

4. L'OUTSOURCING IT: BEST PRACTICE E AUDITING

Sono terminati i lavori del Gruppo di Ricerca AIEA "**L'OUTSOURCING IT: BEST PRACTICE E AUDITING**".

A conclusione delle attività, è stato pubblicato un documento nel quale sono raccolte "alcune best practice pertinenti alla professione dell'IS Auditor quando essa sia esercitata per la revisione di realtà nelle quali il Sistema Informativo, o anche la sola gestione dell’infrastruttura IT, siano stati esternalizzati”.

Riportiamo, di seguito, parte della prefazione del documento.

«*Nel corso della ricerca ed in questo documento abbiamo scelto di evidenziare quegli aspetti che sono emersi dall'esperienza e dalla sensibilità dei componenti del gruppo di lavoro, aspetti che sono stati volutamente privilegiati rispetto alla consuetudine che, in un ambito come questo, ne vorrebbe invece vedere l’esposizione limitata al minimo. Questo lavoro è stato svolto in collaborazione da AIEA e CLUSIT con l'intento di approfondire, come già evidenziato, sia le tematiche proprie dell'attività di Auditing che le tematiche relative alla sicurezza in particolare nella gestione del contratto. Pertanto una particolare attenzione è stata posta agli aspetti legali/contrattuali e agli aspetti della sicurezza, senza i quali risulta difficile una efficace gestione dei rischi di un processo di outsourcing*.»

Il documento è per il momento riservato ai soci AIEA e ai soci CLUSIT, che possono farne richiesta a info@clusit.it. A breve sarà anche organizzato, su tale argomento, un convegno/seminario a cura di AIEA e CLUSIT.

5. NOTIZIE DAI SOCI

Segnaliamo che Louis Vuitton, facente parte del Gruppo LVMH, ricerca per il proprio stabilimento di calzature nella Riviera del Brenta in provincia di Venezia uno/a stagista per i Sistemi Informativi perla durata di 6 mesi a partire da Novembre. La sede di lavoro è Fiesso d'Artico (ve). Il candidato ideale è un neolaureato con competenze teoriche sistemistiche e di networking ed una specializzazione in sicurezza informatica. La posizione comporta lo studio, la definizione, la progettazione, l'ingegnerizzazione di dispositivi e procedure di disaster recovery e di security della filiale italiana di Louis Vuitton. Il progetto si integrerà con il roll out di procedure tecniche dalla casa madre e sistemi informatici. È preferibile una persona che abita in zona Venezia, Padova, Treviso, Vicenza.

Chi fosse interessato può scrivere a info@clusit.it.

Il Vicepresidente dell'Associazione Italiana Intermnet Provider (AIIP), Joy Marino è stato chiamato a partecipare al Comitato sul futuro di Internet, indetto dal Ministro Nicolais per far fronte ai lavori preparatori del forum Atene 2006.

Il Comitato è coordinato dal Professore Stefano Rodotà ed ha come riferimento diretto il Sottosegretario Beatrice Magnolfi. Ne fanno parte Laura Abba (distribuzione di cultura e tecnologie Internet), Vittorio Bertola (servizi Internet), Fiorello Cortiana (standard aperti, diritto d'autore e copyright), Matilde Ferraro (digital divide), Joy Marino (operatori di servizi Internet), Antonino Mazzeo (reti e sicurezza dei sistemi informativi), Stefano Trumpy (sistemi di gestione di Internet). [Fonte: AIIP]

CEFRIEL e MIP Politecnico di Milano ripropongono anche quest'anno la 5a Edizione del Corso di Alta Formazione in Information Security Management, con inizio a Novembre 2006, con due edizioni a Milano e a Roma. Il Corso, che anche per la prossima edizione ha ottenuto il patrocinio del Clusit, riserverà a tutti i soci iscritti al Clusit uno sconto del 10% sulla quota di partecipazione.

L'obiettivo del Corso è di formare esperti a 360° nella gestione di tutte le attività volte a garantire la sicurezza del patrimonio informatico ed informativo di un'azienda (Information Security Manager o Chief Information Security Officer). I destinatari sono responsabili delle aree IT, Organizzazione, Security, di piccole, medie e grandi imprese industriali, di servizi e della Pubblica Amministrazione (e, più in generale, chi ricopre o intende ricoprire in futuro la posizione di CISO), nonché consulenti ICT e di direzione aziendale.

Il percorso formativo, fortemente innovativo nei contenuti e nelle metodologie didattiche, integra le tre aree disciplinari fondamentali d'impatto della sicurezza informatica: technology, management e legal, nonchè un'innovativa sezione dedicata all'intelligence.

Il Corso si articola in sessioni quindicinali nei giorni di venerdì (8 ore) e sabato mattina (4 ore) lungo un arco di circa 8 mesi, per un totale di circa 180 ore, e prevede la realizzazione di un project work di gruppo incentrato su problematiche reali.

La presentazione della nuova edizione del corso avverrà il giorno 3 ottobre p.v., alle ore 17,30, presso la sede del MIP Politecnico di Milano (via Garofalo 39), nell'ambito del seminario "La Gestione delle frodi. L'Information Sharing e il ruolo dell'autorità giudiziaria", in cui è prevista la partecipazione di esponenti della Polizia Postale e delle Comunicazioni e di manager di alcune tra le più importanti aziende di servizi, i quali si confronteranno sul tema dell'Information Sharing tra

le aziende e la necessità di un rapporto strutturato con l'autorità giudiziaria per far fronte al sempre crescente fenomeno delle frodi informatiche. Al termine

saranno consegnati i diplomi agli allievi della 4a edizione, conclusasi nel giugno scorso.

Per ulteriori informazioni: Ciro Marconi, Coordinamento ISM, tel. 02.2399.2881, e-mail: securman@cefriel.it, web site: www.securman.it.

Segnaliamo che l'AIEA ha organizzato un corso di IS Auditing di base a Milano, nella settimana dal 13 al 17 novembre 2006.

Tutte le informazioni utili sono disponibili su www.aiea.it

6. EVENTI SICUREZZA

3 ottobre 2006, Roma Seminario CLUSIT - "Web Applications Security: hands-on lab"

www.clusit.it/edu/index.htm#WS01

3 ottobre 2006, Milano "La Gestione delle frodi. L'Information Sharing e il ruolo dell'autorità giudiziaria"

www.clusit.it/eventi/061003_mip.pdf

4 ottobre 2006, Milano "Elogio della sicurezza"

www.clusit.it/eventi/061004_unicat.pdf

10-12 ottobre 2006, Roma ISSE Conference 2006

www.clusit.it/eventi/061010_isse.pdf

12-13 ottobre 2006, Segrate MI Global Security Conference

http://www-05.ibm.com/services/learning/it/ta-iris.nsf/(extcoursenr)/SC000IT

17 ottobre 2006, Milano

31 ottobre 2006, Roma Seminario CLUSIT - "Il Social Engineering e la sua applicazione nel Penetration Testing professionale"

www.clusit.it/edu/index.htm#SE01

26 ottobre 2006, Roma "Security e Privacy nelle TLC"

www.vonitaly.com

CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*
Dipartimento di Informatica e Comunicazione - Università degli Studi di Milano Via Comelico 39 - 20135 MILANO - cell. 347.2319285

* associazione senza fini di lucro, costituita il 4 luglio 2000